(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 octobre 2005 (06.10.2005)

PCT

(10) Numéro de publication internationale
WO 2005/093994 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/EP2005/050829

(22) Date de dépôt international :
25 février 2005 (25.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0401976 27 février 2004 (27.02.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **GIRARD, Pierre** [FR/FR]; 942, chemin du Tourtaret, F-13112 LA DESTROUSSE (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** DIGITAL CERTIFICATE PRODUCTION METHOD, ASSOCIATED DIGITAL CERTIFICATE, AND METHOD OF USING ONE SUCH CERTIFICATE

(54) **Titre :** PROCEDE DE PRODUCTION D'UN CERTIFICAT NUMERIQUE, ET CERTIFICAT NUMERIQUE ASSOCIE, ET PROCEDE D'UTILISATION D'UN TEL CERTIFICAT NUMERIQUE

(57) **Abstract:** The invention relates to a method of producing a digital certificate, during which a certificate authority (i) compiles a data set containing a public key and digital data comprising data identifying the owner of said public key and an associated private key, and subsequently (ii) signs the data set in order to produce a digital certificate. According to the invention, the digital data also comprise data that identify means for generating the private key and/or means for storing the private key on a support and/or means for signing with the private key. The invention can be used to produce X509-type digital certificates.

(57) **Abrégé :** L'invention concerne un procédé de production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble de données pour produire un certificat numérique. Selon l'invention, les données numériques comprennent également des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée. Application à la réalisation de certifiifcats numériques de type X509.

WO 2005/093994 A1

PROCEDE DE PRODUCTION D'UN CERTIFICAT NUMERIQUE, ET CERTIFICAT NUMERIQUE ASSOCIE, ET PROCEDE D'UTILISATION D'UN TEL CERTIFICAT NUMERIQUE

Dans le domaine des transactions électroniques sécurisées, l'invention concerne plus particulièrement la production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble des données pour produire un certificat numérique.

Par transaction électronique, on entend ici une transmission d'un ensemble de données numériques (ensemble qu'on appellera message ou message électronique par souci de simplicité) dans le sens le plus large. Il peut s'agir par exemple de la transmission d'un acte d'achat ou de vente, de la transmission d'une demande d'accès à un service en ligne, de la transmission d'un message d'information signé électroniquement, etc.

De telles transactions peuvent être sécurisées par l'utilisation d'algorithmes de chiffrement et / ou de signature (par exemple l'algorithme RSA) à clés asymétriques : une clé privée et une clé publique.

La clé privée est utilisée par l'émetteur pour signer un message avant envoi. La clé privée est une caractéristique de la personne qui émet un message signé, elle est conservée secrète, par exemple dans une mémoire d'un matériel propriété de l'émetteur du message. La clé privée peut ainsi être conservée sur un disque interne

d'un ordinateur personnel, dans une mémoire d'une carte SIM (Subscriber Identification Module ou module d'identification d'abonnés) d'un téléphone portable, dans une mémoire d'une carte à mémoire ou d'une carte à microprocesseur accessible en lecture par un ordinateur personnel par l'intermédiaire d'un lecteur de carte, etc.

La clé publique est utilisée par la personne qui reçoit le message, pour vérifier l'authenticité du message signé reçu et l'identité de l'émetteur du message reçu.

L'utilisation d'algorithmes de signature suppose, préalablement à toute transaction, que l'émetteur communique sa clé publique à la personne destinataire de la transaction. Cette communication peut être directe : envoi d'un message contenant la clé, envoi d'un support physique tel qu'une mémoire ou un disque sur lequel est mémorisée la clé, etc. Cette communication peut se faire également par l'intermédiaire d'une infrastructure de clé publique (ou PKI pour Public Key Infrastructure en anglais) ou infrastructure de certification.

Une infrastructure de clé publique fait intervenir notamment une entité de certification et un tiers certificateur, pour permettre une cohérence dans la gestion des couples de clés.

L'entité de certification est un organisme normatif qui définit notamment les conditions de certification, les données devant être incluses dans un certificat et la manière dont sont utilisés les certificats produits. De manière connue, un certificat comprend une clé publique et des données identifiant un ou plusieurs propriétaires de la dite clé publique et de la clé privée associée.

Le mot propriétaire doit être ici compris au sens large.

Le propriétaire des clés peut bien sûr être une personne physique. Mais le propriétaire peut également être un matériel auquel est attachée le couple de clé. Par exemple, dans une société de grande taille, propriétaire de plusieurs serveurs de transmissions de données numériques, il est fréquent qu'un ou plusieurs serveurs "possèdent" leurs propres clés.

Aussi, et selon les consignes de l'entité de certification, les données identifiant chaque propriétaire peuvent comprendre le nom de l'utilisateur et / ou son adresse postale et / ou ses coordonnées bancaires et / ou des numéros de carte d'identité et / ou des références identifiant un matériel propriétaire.

Un des formats de certificat couramment utilisé est le format X509, défini selon la norme Information technology - Open Systems Interconnection - The Directory : Public-Key and attribute certificate frameworks datée de Mars 2002 de l'International Telecomunication Union. Le format X509 comprenant, pour chaque certificat, les paramètres suivants :

- un numéro de référence associé au certificat
- une indication du procédé utilisé pour la signature numérique d'un message,
- les coordonnées de l'émetteur du certificat,
- la période de validité du certificat,
- les coordonnées du propriétaire de la clé
- la clé publique
- un ensemble de N champs libres d'utilisation
- la signature de l'émetteur du certificat

Le tiers certificateur émet les certificats numériques et les met à disposition du public pour consultation dans une base de données regroupant un ensemble de certificats. Le tiers certificateur est ainsi chargé dans

un premier temps de collecter et vérifier les informations devant figurer dans un certificat. Dans un deuxième temps, le tiers certificateur regroupe la clé publique et les données identifiant le propriétaire de la dite clé publique dans un message numérique qu'il signe avec sa propre clé privée pour former le certificat numérique. Enfin, le tiers certificateur met le certificat à disposition dans une base de données.

En consultant la base de certificats, et si elle fait confiance au tiers certificateur, une personne va pouvoir authentifier l'émetteur d'un message signé qu'elle a reçu ou chiffrer un message à sa destination, avant de valider ou non une vente, d'autoriser ou non l'accès à un site réservé aux abonnés, etc.

Les techniques de production et de mise à disposition de certificats numériques sont aujourd'hui assez répandues. Elles ont permis de sécuriser dans une certaine mesure les transactions électroniques pour permettre leur développement. L'intervention d'un tiers certificateur, l'utilisation d'algorithmes cryptographiques et de protocoles sécurisés pour l'obtention des certificats permet de garantir l'identité de la personne qui a demandé un certificat sur la base de sa clé publique.

Toutefois, un certificat ne garantit pas qu'un message reçu a été signé par le propriétaire de la clé privée associée à la clé publique et utilisée pour la signature du message reçu. Plus précisément, un certificat ne garantit pas qu'une clé privée utilisée pour la signature d'un message n'a pas été dérobée ou utilisée à l'insu de son propriétaire.

Stockée sur un ordinateur personnel, la clé privée est susceptible d'être dérobée ou modifiée ou utilisée à

l'insu de son propriétaire par un tiers malveillant, par exemple par l'intermédiaire d'un virus ou d'un cheval de Troie. Pour éviter ce risque, des matériels spécifiques, tels que des cartes à mémoire associées à un lecteur de carte, ont été développés pour mémoriser notamment les clés privées ; un risque demeure toutefois lorsque la clé privée est lue dans la carte et transmise à un programme de signature présent dans l'ordinateur personnel. Pour limiter encore ce risque, des cartes à microprocesseur ont été développées, qui mémorisent non seulement la clé privée, mais également le procédé de signature utilisant la dite clé privée, de sorte que la clé privée n'est jamais accessible directement depuis l'extérieur, par exemple sur une borne d'entrée / sortie de la carte.

Ainsi, certains des matériels et des procédés actuels permettent le renforcement voire la suppression des risques de vol ou de l'usage d'une clé privée à l'insu de son propriétaire.

Toutefois, un tiers distant, qui a accès seulement à un certificat associé à la clé privée, ne sait pas estimer le risque qu'il prend en acceptant la signature électronique d'un utilisateur distant. Ceci limite bien sûr le degré de confiance qu'un tiers peut avoir dans un certificat numérique ou dans un message signé reçu.

L'invention a pour but de résoudre ce problème en proposant un procédé de production d'un certificat et un certificat associé contenant des informations permettant à un tiers qui reçoit un message signé d'estimer la probabilité pour que l'émetteur de la transaction soit bien le propriétaire authentique de la clé privée utilisée pour la signature.

Pour cela l'invention propose un procédé de production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble de données pour produire un certificat numérique.

Selon l'invention, le procédé est caractérisé en ce que les données numériques comprennent également des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée.

Les données identifiant les moyens de génération de la clé privée pourront par exemple comprendre des données identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée.

Les données identifiant les moyens de mémorisation de la clé privée pourront quant à eux comprendre des données identifiant :

- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée.

Enfin, les données identifiant les moyens de signature pourront par exemple comprendre des données identifiant :

- un procédé de signature utilisant la clé privée,
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

Les données identifiant un matériel ou un support de mémorisation comprennent par exemple :

- une référence identifiant le dit matériel ou le dit support de mémorisation et / ou
- une identification d'un fabricant du dit matériel ou du dit support de mémorisation et / ou
- une indication d'un niveau de sécurité du dit matériel ou du dit support de mémorisation défini selon une norme ISO15408 datée du 01/12/1999.

Les données identifiant un procédé comprennent :

- une référence identifiant le dit procédé et / ou
- une identification d'un inventeur du dit procédé et / ou
- une indication d'un niveau de sécurité du dit procédé selon la norme ISO 15408.

Les données identifiant un lieu comprennent :

- une identification du dit lieu et / ou
- une indication d'un niveau de sécurité du dit lieu selon la norme ISO 15408.

L'invention concerne également un certificat numérique comprenant :

- une clé publique,
- des données identifiant un propriétaire de la clé publique et d'une clé privée associée, et
- des données identifiant des moyens de génération de

la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la dite clé privée.

Dans un mode de réalisation préférée le certificat est de type X509 selon une norme Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks datée de Mars 2000 de l'International Telecomunication Union. Dans le certificat X509, un ensemble de champs prédéfinis et libres sont utilisés pour mémoriser les données numériques identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée et / ou
- un procédé de signature utilisant la clé privée et / ou
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

L'invention concerne également un procédé d'utilisation d'un certificat numérique tel que décrit ci-dessus, comprenant les étapes suivantes consistant à :

- recevoir un message signé avec une clé privée,
- lire, dans le certificat numérique, des données identifiant des moyens de génération de la clé privée

et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée,

- en déduire une probabilité pour que la dite clé privée ait été utilisée par un propriétaire légitime de ladite clé privée,
- en fonction de la dite probabilité, accepter ou refuser le message électronique.

On peut par exemple choisir d'accepter un message uniquement si la probabilité pour que la dite clé ait été utilisée par son propriétaire légitime est supérieur à une valeur prédéfinie VB. La valeur prédéfinie est choisie en fonction du niveau de sécurité souhaité pour une transaction. On pourra par exemple choisir une valeur prédéfinie proportionnelle aux enjeux financiers liés à une transaction.

On peut aussi choisir de :

- accepter le message si la probabilité est supérieure à une première valeur VB1,
- demander une confirmation de la transaction si la probabilité est comprise entre la première valeur VB1 et une deuxième valeur VB2 inférieure à la première, et
- refuser le message si la probabilité est inférieure à la deuxième valeur.

Pour estimer la probabilité pour que la clé privée ait été utilisée par son propriétaire légitime, on utilise les informations relatives à la clé secrète présentes dans le certificat numérique.

Dans un exemple, les informations présentes dans le certificat et relatives à la clé privée indiquent que la clé privée a été générée et mémorisée dans une carte à microprocesseur qui mémorise également un procédé de

signature. Les informations relatives à la clé privée indiquent également que la génération de la clé, sa mémorisation et la mémorisation du procédé de signature ont été réalisés au sein même de l'usine qui a fabriqué la carte, usine possédant un niveau de certification (en terme de sécurité) maximal. Dans ce cas, un tiers qui consulte le dit certificat sait que la probabilité est maximale (et supérieure à la valeur prédéfinie) pour que la clé privée ait été utilisée par son propriétaire légitime et il peut en déduire avec quasi-certitude l'identité de l'émetteur d'une transaction signée qu'il a reçue.

Dans un autre exemple, les informations présentes dans le certificat et relatives à la clé privée indiquent que la clé privée a été générée dans un point de vente de matériel informatique, et que la clé privée et le procédé de signature sont mémorisés sur un disque dur d'un ordinateur personnel. Dans ce cas, un tiers qui consulte le dit certificat sait que la probabilité est forte pour que la clé privée ait pu être subtilisée ou utilisée à l'insu de son propriétaire. Il peut en déduire que l'identité de l'émetteur d'une transaction signée qu'il a reçue n'est pas certaine et en conséquence, décider de refuser la transaction pour éviter un risque.

REVENDICATIONS

1. Procédé de production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble de données pour produire un certificat numérique,

le procédé étant caractérisé en ce que les données numériques comprennent également des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée.

2. Procédé selon la revendication 1, dans lequel les données identifiant les moyens de génération de la clé privée comprennent des données identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée.

3. Procédé selon la revendication 1 ou 2, dans lequel les données identifiant les moyens de mémorisation de la clé privée comprennent des données identifiant :

- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou

- un support de mémorisation sur lequel est mémorisée la clé privée.

4. Procédé selon l'une des revendications 1 à 3, dans lequel les données identifiant les moyens de signature comprennent des données identifiant :
- un procédé de signature utilisant la clé privée,
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

5. Procédé selon l'une des revendications 2 à 4, dans lequel les données identifiant un matériel ou un support de mémorisation comprennent :
- une référence identifiant le dit matériel ou le dit support de mémorisation et / ou
- une identification d'un fabricant du dit matériel ou du dit support de mémorisation et / ou
- une indication d'un niveau de sécurité du dit matériel ou du dit support de mémorisation défini selon une norme ISO15408.

6. Procédé selon l'une des revendications 2 à 5, dans lequel les données identifiant un procédé comprennent :
- une référence identifiant le dit procédé et / ou
- une identification d'un inventeur du dit procédé et / ou
- une indication d'un niveau de sécurité du dit procédé selon la norme ISO 15408.

7. Procédé selon l'une des revendications 2 à 6, dans lequel les données identifiant un lieu comprennent :
- une identification du dit lieu et / ou
- une indication d'un niveau de sécurité du dit lieu selon la norme ISO 15408.

8. Certificat numérique comprenant :

- une clé publique,
- des données identifiant un propriétaire de la clé publique et d'une clé privée associée, et
- des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la dite clé privée.

9. Certificat selon la revendication 8, de type X509 selon une norme Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks datée de Mars 2000 de l'International Telecomunication Union , dans lequel un ensemble de champs prédéfinis et libres sont utilisés pour mémoriser les données numériques identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée et / ou
- un procédé de signature utilisant la clé privée et / ou
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

10. Procédé d'utilisation d'un certificat numérique selon l'une des revendications 8 ou 9, comprenant les étapes suivantes consistant à :

- recevoir un message signé avec une clé privée,
- lire, dans le certificat numérique, des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée,
- en déduire une probabilité pour que la dite clé privée ait été utilisée par un propriétaire légitime de ladite clé privée,
- en fonction de la dite probabilité, accepter ou refuser le message électronique.

11. Procédé selon la revendication 10, dans lequel le message est accepté uniquement si la probabilité pour que la dite clé ait été utilisée par son propriétaire légitime est supérieur à une valeur prédéfinie.

12. Procédé selon la revendication 10, dans lequel :
- on accepte un message si la probabilité est supérieure à une première valeur (VB1),
- on demande une confirmation du dit message si la probabilité est comprise entre la première valeur (VB1) et une deuxième valeur (VB2) inférieure à la première valeur, et
- on refuse le message si la probabilité est inférieure à la deuxième valeur (VB2).

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/050829

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/115457 A1 (ANSELL STEPHEN M ET AL) 19 June 2003 (2003-06-19)	1-9
A	abstract paragraphs '0004! - '0010! paragraph '0019! paragraphs '0024!, '0025! paragraph '0027! paragraphs '0032!, '0033! figure 5	10-12
A	EP 0 869 637 A (ARCANVS) 7 October 1998 (1998-10-07) abstract page 3, line 25 - line 56 page 5, line 49 - page 6, line 8 figures 2-11	1-12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 June 2005	08/06/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bec, T

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/050829

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003115457 A1	19-06-2003	CA 2365441 A1	19-06-2003
EP 0869637 A	07-10-1998	EP 0869637 A2	07-10-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2005/050829

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2003/115457 A1 (ANSELL STEPHEN M ET AL) 19 juin 2003 (2003-06-19)	1-9
A	abrégé alinéas '0004! - '0010! alinéa '0019! alinéas '0024!, '0025! alinéa '0027! alinéas '0032!, '0033! figure 5	10-12
A	EP 0 869 637 A (ARCANVS) 7 octobre 1998 (1998-10-07) abrégé page 3, ligne 25 - ligne 56 page 5, ligne 49 - page 6, ligne 8 figures 2-11	1-12

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
1 juin 2005	08/06/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bec, T

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/EP2005/050829

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003115457 A1	19-06-2003	CA 2365441 A1	19-06-2003
EP 0869637 A	07-10-1998	EP 0869637 A2	07-10-1998